NLECTC NIJ

Criminal Justice
Electronic Crime Technology
Center of Excellence

EnCase® Portable

EVALUATION REPORT

August 2011

NIJ Criminal Justice Electronic Crime Technology Center of Excellence
550 Marshall St., Suite B
Phillipsburg, NJ 08865
www.ECTCoE.org

NIJ ECTCOE TESTING AND EVALUATION PROJECT STAFF

Robert J. O'Leary, CFCE; DFCP
Russell Yawn, CFCE
Laurie Ann O'Leary
Michael Terminelli
Donald Stewart, CFCE
Randy Becker, CFCE
Mark Davis, Ph.D
Victor Fay-Wolfe, Ph.D
Chester Hosmer

Table of Contents

Introduction

The National Institute of Justice (NIJ) Electronic Crime Technology Center of Excellence (ECTCoE) has been assigned the responsibility of conducting electronic crime and digital evidence tool, technology and training testing and evaluations in support of the NIJ research, development, testing and evaluation (RDT&E) process.

The NIJ RDT&E process helps ensure that NIJ's research portfolios are aligned to best address the technology needs of the criminal justice community. This rigorous process has five phases:

- **Phase I. Determine technology needs, principally in partnership with the Law Enforcement and Corrections Technology Advisory Council (LECTAC) and the appropriate Technology Working Group (TWG).** NIJ identifies criminal justice practitioners' functional requirements for new tools and technologies. (For more information on LECTAC and the TWGs, visit http://www.justnet.org/.)
- **Phase II: Develop technology program plans to address those needs.** NIJ creates a multi-year research program to address the needs identified in Phase I. One of the first steps is to determine whether products that meet those needs currently exist or whether they must be developed. If a solution is already available, Phases II and III are not necessary and NIJ moves directly to demonstration, testing and evaluation in Phase IV. If solutions do not currently exist, they are solicited through annual, competitively awarded science and technology solicitations and TWG members help review the applications.
- **Phase III: Develop solutions.** Appropriate solicitations are developed and grantees are selected through an open, competitive, peer-reviewed process. After grants are awarded, the grantee and the NIJ program manager then work collaboratively to develop solutions.
- **Phase IV: Demonstrate, test, evaluate and adopt potential solutions into practice.** A potential solution is tested to determine how well it addresses the intended functional requirement. NIJ then works with first-adopting agencies to facilitate the introduction of the solution into practice. During the testing and evaluation process, performance standards and guides are developed (as appropriate) to ensure safety and effectiveness; not all new solutions will require the publication of new standards or guides. After adoption, the solution's impact on practice is evaluated.
- **Phase V: Build capacity and conduct outreach to ensure that the new tool or technology benefits practitioners.** NIJ publishes guides and standards and provides technology assistance to second adopters.[1]

NIJ's High-Priority Criminal Justice Technology Needs are organized into five functional areas:

- Protecting the Public.
- Ensuring Officer Safety.
- Confirming the Guilty and Protecting the Innocent.
- Improving the Efficiency of Justice.
- Enabling Informed Decision-Making

These NIJ ECTCoE tool, technology and training evaluation and testing reports support the NIJ RDT&E process, which addresses high-priority needs for criminal justice technology.

[1] *National Institute of Justice High-Priority Criminal Justice Technology Needs,* March 2009, NCJ 225375.

Overview

The increasing demand to collect volatile data from computers in the field often exceeds the human and technology resources of most organizations and agencies. There is a clear need for a technology solution that increases the productivity and utility of a wider range of personnel, making them proficient in data collection.

EnCase Portable is a pocket-sized USB data collection and triage solution that leverages the powerful capabilities of EnCase®. Unlike other solutions, EnCase Portable can be used by non-experts enabling the limited number of computer forensic examination specialists to focus on case management, processing, detailed analysis and reporting.

Product Information

The following is product information contained in the EnCase Portable 2.1 brochure:

The EnCase Portable solution can be configured to automatically search a targeted computer and collect data, including documents, Internet history and artifacts, images, other digital evidence and even entire hard drives. During this search and collection, images, documents, Internet history and a variety of other data can be reviewed in real time on the target computer. The combination of these two critical abilities—collection and triage—in one easy-to-use solution enables unsurpassed efficiency and effectiveness.

With EnCase Portable, organizations of any size, in any industry, can increase their ability to capture data, utilizing virtually everyone in their organization in the data collection and triage process. With the non-experts in the field collecting data, specialists in forensic investigations, eDiscovery and Cybersecurity investigators can remain focused on analysis and processing, closing cases and securing networks:

- The expert configures EnCase Portable to meet specific collection or triage requests.
- The non-expert runs EnCase Portable in the field to search, review and collect relevant data.
- Collected data is sent back to the expert for further analysis/processing using EnCase.
- According to the documentation in the EnCase Portable Manual, EnCase Portable enables a person familiar with EnCase to create search, collection and triage jobs using keywords, file types, dates, etc., as the criteria. Once created, the jobs can be published to the EnCase Portable device and used by anyone to execute the job. This unsurpassed flexibility means that EnCase Portable can handle any situation that arises.
- The EnCase Portable user can then insert the device into a target computer in the field, select the job and EnCase Portable will do the rest. With EnCase Portable, you can perform a targeted or broad collection, even of an entire hard drive, with ease. During a triage job, the user may review images, documents, Internet history and a variety of other data in real time on the target computer while the search is in progress.

Product Description

The following is a description of EnCase Portable from Guidance Software's website[2]:

EnCase Portable is a pocket-sized USB data collection and triage solution that leverages the powerful

[2] http://www.guidancesoftware.com/EnCase-portable.htm

capabilities of EnCase®. Unlike other solutions, EnCase Portable can be used by non-experts, enabling scarce specialist resources to focus on case management, processing, detailed analysis and reporting.

The solution automatically searches a targeted computer and collects data, including documents, Internet history and artifacts, images, other digital evidence and even entire hard drives. During this search and collection, images, documents, Internet history and a variety of other data can be reviewed in real time on the target computer. The combination of these two critical abilities — collection and triage — in one easy-to-use solution enables unsurpassed efficiency and effectiveness.

Special Features

The following is a list of special features of EnCase Portable, provided by Guidance Software's website:

Key Benefits:

- Creates a repeatable and defensible collection process using non-technical personnel.
- Triages suspect computers instantly.
- Preserves digital evidence in the court-vetted evidence file format for which EnCase is known.
- Collects data in remote locations without sending expert personnel.
- Seamlessly integrates collected data into EnCase® Forensic or EnCase® Enterprise for analysis.
- Ultra-portable.

Key Features:

- Uses Keywords and Hash values to perform targeted collections.
- Instantly views images on the target computer.
- Live and turned off computer operating modes.
- Customizable search, triage and collection jobs.
- Searches and collects without leaving a trace on the target computer.

Target Customers

The target customers of EnCase Portable, according to Guidance Software, are:

- Law enforcement personnel.
- Civilian investigators.
- Military personnel.
- Government personnel.
- IT professionals.
- Law firm personnel.
- Litigation support personnel.
- Service provider personnel.
- Non-technical personnel.

Law Enforcement Applications

EnCase Portable can be used in a law enforcement setting to extract potential digital evidence from a computer at the scene. EnCase Portable is designed to be simple to use, enabling a law enforcement professional who may not be highly trained in digital forensics processing to acquire potential digital evidence. This evidence can later be examined by a trained digital evidence investigator.

Evaluation and Testing of EnCase Portable

Test Bed Configuration

To prepare for testing and evaluation of EnCase Portable, staff designed and configured a test bed to simulate realistic conditions. Having knowledge of what "evidence" exists on the test bed enables easy evaluation of EnCase Portable. The test bed is located at the Electronic Crime Technology Center of Excellence Lab, 550 Marshall St., Ste. B, Phillipsburg, NJ 08865. The following is a list of the systems used for testing and their configuration details:

- Computers
  - Gateway Mid Tower PC (Gateway Test PC)
    - Model number: MFATXSL KTA 300SE.
    - Serial number: 0026280320.
    - MFG DATE: 2/15/2002.
    - Intel 400075P motherboard.
    - Intel Celeron 1200 MHz, 1.2 GHz.
    - 512 MB Ram installed.
    - DVD/CD reader.
    - 3.5 Inch floppy drive
- Lab Computer 2
  - This computer was used to interact with the Gateway Test PC. Since it was not used to directly test EnCase Portable, its hardware details are not included here.
  - This computer was prepared with Limeware installed and shared files "Mov15D.avi," "action video ectcoe.avi," "my home videos ectcoe.avi," "joker1.jpg" and "joker2.jpg."
- Hard Drive
  - Western Digital WD200 20GB Model Number: WD200BB-75CAA0.
  - Serial number: WMA8J1826063.
  - DCM: HSEHNA2AB.
  - MFG Date: 6 MAR 2002.
  - Wiped with SPADA disk wiping utility.
  - Checksum performed on wiped hard drive:
    - Time & Date: 06:52hrs 20 Aug 2010.
    - Device checked/dev/hda.
    - CKSUM64 Checksum – 0000000000000000:
    - Read 610359 records + 24576 bytes (total of 20000268288 bytes) (total of 39063024 sectors).
    - Wrote 0 records + 0 bytes (total of 0 bytes) (total of 0 sectors).
    - Total time 503.161sec (38817 kBytes/sec).
- Operating system: Microsoft XP Home Edition
  - The operating system, Microsoft XP Home Edition Version 2002, (55277-OEM-0011903-00105) was installed from the OEM CD-ROM supplied by Gateway. A standard installation was performed, the time zone set for eastern United States and Canada, and service pack 3 and all pending updates were installed.
- User accounts and computer name configuration
  - The Gateway Test PC was named "Test Computer 1" with the owner set to "ECTCoE." The following users were configured on the computer:

User	Type	Password
LABXPGTWY1	Administrator	ectcoe
Alice	Limited User	testpass
Bill	Limited User	<BLANK>
Charlie	Limited User	<BLANK>

- Additional programs and configuration
  - Avast Free Anti VirusVersion 5.0.594, Virus definitions 100820.0 created Aug. 20, 10, at 5:02 a.m.
  - Gmail accounts created on Gateway Test PC on Aug. 23, 2010:

User	Email	Password
Alice Smith	smitha550@gmail.com	coffee01
Bill Jones	billj020@gmail.com	coffee01
Charlie Kline	charliekline121@gmail.com	coffee01

  - Performed all of the pending operating system, Microsoft Internet Explorer and driver updates from the "labxpgtwy1" administrator account. All of the updates were completed on Aug. 24, 2010, and the computer was restarted.
  - Limewire v5.5.14[3]:
    - When the LimeWire username on the sharing computer is not specified, LimeWire assigns a username using a numeric to alpha character dictionary translating the first two octets of the IP address into the alpha portion of the LimeWire username, which is appended with the numerical value of the last two octets of the IP address.
    - The LimeWire numeric to alpha character dictionary translates the IP address 192.168 to "magicmushroom" and appends the remainder of the IP address 20.100 to create the LimeWire username sharing files.
- Test data set
  - Photographs of playing cards were created to serve as a test data set. The files were named using the convention "<face value of the card>_<card suite>" (e.g., "ace_hearts.jpg"). These files were then saved to a Kingston Data Traveler 4GB USB thumb drive.
- Normal usage simulation
  - Several actions were performed on the Gateway test computer to simulate normal usage. The details of these actions follow:
    - The Alice account was logged into at 7:25 a.m. on Aug. 24, 2010.
    - The Kingston Data Traveler 4GB USB thumb drive was inserted at 7:25 a.m. and photograph image files of the 13 Diamond suite playing cards were copied into the Alice user account "My Pictures" folder located in the "My Documents" folder.
    - Microsoft Internet Explorer was opened at 7:29 a.m.
    - The Google website, www.google.com, was accessed at 7:30 a.m.
    - The Gmail link was accessed and the smitha550@gmail.com Gmail account was opened at 7:30 a.m. and the following actions were performed:
      - An e-mail message was sent at 7:37 a.m. to Bill regarding a staff meeting on Aug. 25, 2010 at 9 a.m.
      - An e-mail message was sent at 7:37 a.m. to an incorrect address to Charlie's Gmail account regarding a staff meeting on Aug. 25, 2010 at 9 a.m. in anticipation of generating an error message.
    - Alice received an e-mail reply that the incorrect e-mail address for Charlie was not found.
    - The staff meeting e-mail was sent to the correct Gmail account for Charlie at 7:38 a.m.

[3] http://wiki.limewire.org/index.php?title=LW_5_FAQ

- At 7:40 a.m. on Aug. 24, 2010, the Gmail calendar for the Alice account was opened and an appointment for a staff meeting at 9 a.m. on Aug. 25, 2010, was entered. Alice then shared the Gmail calendar with Bill and Charlie at 7:42 a.m.
- Logged off the Alice Gmail account at 7:43 a.m.
- Logged off the computer at 7:44 a.m.
- Logged onto the Bill user account at 7:44 a.m.
- The 13 Club suite playing cards were copied from the Kingston Data Traveler thumb drive to the user account Bill's "My Pictures" folder at 7:46 a.m.
- Microsoft Internet Explorer was opened at 7:47 a.m.
- The Google website, www.google.com, was accessed at 7:48 a.m.
  - The Gmail link was accessed and the billj020@gmail.com Gmail account was opened at 7:48 a.m. and the following actions were performed:
  - Read all e-mails, replied to Alice at 7:49 a.m.
  - Responded to calendar invite 7:51 a.m.
  - Logged off Gmail.
- Logged Bill out of computer 7:53 a.m.
- Logged onto the Charlie user account at 7:54 a.m.
- At 7:55 a.m., using the same Kingston Data Traveler thumb drive still plugged into the computer, the 13 Heart suite playing cards were copied into the user account Charlie's "My Pictures" folder.
- Microsoft Internet Explorer was opened at 7:56 a.m.
- The Google website, www.google.com, was accessed at 7:56 a.m.
  - The Gmail link was accessed and the charliekline121@gmail.com Gmail account was opened at 7:56 a.m. and the following actions were performed:
  - Read all e-mails at 7:58 a.m.
  - Replied to Alice at 7:59 a.m.
  - Responded to calendar invite at 8 a.m.
  - Logged off Gmail.
- Logged off the Charlie user account at 8:01 a.m.

- Steps performed for the installation of LimeWire:
  - Logged into the system as LABXPGTWY1 (administrator account).
  - LimeWire v5.5.14 was installed on the test Gateway computer using the USB Kingston Data Traveler thumb drive already inserted into the Test Gateway computer at 11:51 a.m.
  - Installed FrostWire v4.20.9 onto the test computer at 11:56 a.m.
  - Each user account was checked to confirm that a LimeWire folder had been installed. The LimeWire folder is located in the My Documents folder of each user account and contains a "Saved" and an "Incomplete" folder.
  - Logged off LABXPGTWXY1 (administrator account).
  - The Kingston Data Traveler was removed from the test computer.
- Logged on as user Alice and opened the LimeWire program.
  - User Alice shares the file "ace_diamond.jpg" using the LimeWire program at 12:50 p.m.

- Using Lab Computer 2, configured with the same version of LimeWire, a search was conducted for "ace_diamond.jpg." The "ace_diamond.jpg" file was identified as shared by one user, "magicmushroom-20-100."
- From Lab Computer 2, it was determined the IP (Internet Protocol) address of the computer sharing the file was 192.168.20.100.
- From the Gateway Test PC, it was determined that the IP address of Gateway Test PC was 192.168.20.100.
- These checks verified the Limewire user name is based on the IP address of the computer sharing the file.
- The file "ace_diamond.jpg" was downloaded to Test Computer 2 at 1:02 p.m.
- Closed all open applications and logged off Alice user account.

❑ Logged onto the Bill user account at 1:46 p.m.

- Opened the LimeWire program and shared the "ace_club.jpg," "king_club.jpg," "queen_club.jpg" and "jack_club.jpg" files at 1:50 p.m.
- Using Lab Computer 2, conducted a search for the "ace_club.jpg," "king_club.jpg," "queen_club.jpg" and "jack_club.jpg" files at 1:54 p.m.
- The files were found to be shared by username "magicmushroom-20-100," the same username that had previously been assigned to the Alice user account on the Gateway Test computer with the same IP address.
- The four files shared by Bill were downloaded to Lab Computer 2 at 1:57 p.m.
- Logged off the Bill user account.

❑ Using Lab Computer 2, the files "Mov15D.avi,, "action video ectcoe.avi," "my home videos ectcoe.avi," "joker1.jpg" and "joker2.jpg" were shared to the public share in LimeWire.

❑ Logged onto the Alice user account and performed the following actions:

- Started LimeWire.
- Using LimeWire a search was done for "mov15D.avi." The file "mov15D.avi" was found and being shared by "Magicmushroom-20.102."
- Using the LimeWire option to browse files shared by "Magicmushroom-20-102," the other shared files, "action video ectcoe.avi," "my home videos ectcoe.avi," "joker1.jpg," and "joker2.jpg" were identified.
- Downloaded "mov15D.avi," "action video ectcoe.avi" and "joker2.jpg" to Gateway Test PC.
- Checked the directory to determine that the files were indeed downloaded to Alice's "My Documents\LimeWire\Saved" folder.
- Logged off the Alice user account.

❑ Logged onto the Bill user account and performed the following actions:

- Started LimeWire.
- Using LimeWire, a search was conducted for the file "mov15D.avi," which was found to be shared by "Magicmushroom-20.102."
- Using the LimeWire option to browse files shared by "Magicmushroom-20-102," the other shared files "action video ectcoe.avi," "my home videos ectcoe.avi," "joker1.jpg" and "joker2.jpg" were identified.
- User Bill downloaded "mov15D.avi" and "my home videos ectcoe.avi."
- Verification was made that the files were downloaded to Bill user account "My Documents\LimeWire\Saved" folder.
- Logged off the Bill user account.

- Logged onto the Charlie user account and performed the following actions:
  - Using LimeWire, a search was conducted for the file "mov15D.avi," which was found to be shared by "Magicmushroom-20.102."
  - Using the LimeWire option to browse files shared by "Magicmushroom-20-102," the other shared files "action video ectcoe.avi," "my home videos ectcoe.av,i" "joker1.jpg" and "joker2.jpg" were located.
  - User Charlie downloaded all the files contained in the "Magicmushroom-20-102" public share folder.
  - Verification was made that all five shared files were downloaded to Charlie user account "My Documents\LimeWire\Saved" folder.
  - Logged off the Charlie user account.
- The computer was then powered off.
- The test computer was powered on at 6:20 a.m. and the administrator account LABXPGTWY1 was logged onto at 6:30 a.m. on Aug. 25, 2010. The following actions were then performed:
  - The 4GB Kingston Data Traveler thumb drive was inserted into the front USB port of the test computer. The thumb drive contained 11 additional digital image files that were copied to the "My Pictures" folder of all three users.
  - Three digital image files were copied to the Alice's "My Pictures" folder, four were copied to Bill's "My Pictures" folder and the remaining four were copied to Charlie's "My Pictures" folder. All the pictures were copied between 6:31 a.m. and 6:34 a.m.
  - Operating system updates and the antivirus definitions were downloaded and installed at 6:37 a.m., completing at 6:54 a.m.
  - The user account Charlie and all of its associated files was deleted using the "Account Manager" in Microsoft Windows XP at 6:37 a.m.
  - The Kingston Data Traveler was removed from the test computer.
  - The test computer was powered off at 7:02 a.m.
  - Additional setup of Gateway Computer Test Bed on Aug. 27, 2010:
  - The Gateway Test PC was started with the hard drive installed at 7:05 a.m.
  - The administrator account LABXPCTWY1 was logged into at 7:06 a.m.
  - The Kingston Data Traveler thumb drive was inserted into the front USB port at 7:07 a.m.
  - Sixteen documents and 130 digital images were copied to both Alice's and Bill's "My Documents" and "My Pictures" folders, respectively. Additionally, a document containing generic personal information named "Credit cards and SS numbers.txt" was copied to the "My Documents" folder of Bill. This step was completed between 7:07 a.m. and 7:21 a.m.
  - The Kingston Data Traveler was removed from the test computer.
  - Logged off the LABXPGTWY1 administrator account and performed a proper shutdown of the test computer at 7:25 a.m.
- Logged onto the Alice user account and configured Outlook Express 6 Version 6.00.2900.5512 to receive and send e-mail using the smitha550@gmail.com Gmail account and downloaded all incoming e-mail to the inbox at 7:26 a.m.
  - Logged off the Alice user account at 7:45 a.m.
- Logged onto the Bill user account and configured Outlook Express 6 Version 6.00.2900.5512 to receive and send e-mail using the billj020@

gmail.com Gmail account and downloaded all incoming e-mail to the inbox at 7:45 a.m.

- Using Outlook Express 6, sent e-mails to Alice from Bill, including a picture file attachment "dsc00847," between 7:52 a.m. and 7:54 a.m.
- Logged off Bill at 7:55 a.m.

❑ Logged onto the Alice user account at 7:56 a.m.

- Opened Outlook Express and read e-mail from Bill at 7:57 a.m.
- Saved attachment "dsc00847" to desktop at 7:58 a.m.
- Logged off Alice and powered down the Gateway Test bed computer at 7:59 a.m.

■ Creation of cloned "Test Set" hard drives:

❑ Three 20GB Western Digital hard drives, similar to the hard drive on the Gateway Test PC, were used to create cloned drives with the Tableau TD1 Forensics Duplicator. One disk contained a raw image, created with the program "dd," and the other two were created using the drive to drive copy function of the TD1. The hash values of each of the cloned hard drives and the image file were performed and verified to match the hash value of the original test bed hard drive.

Evaluation and Testing

Testing of EnCase Portable was performed in three phases:

■ The first phase is a pre-test designed to familiarize the use of EnCase Portable Version 2.2. This test was also designed to determine if the prepared test bed has sufficient information to complete the scenario testing as outlined in the EnCase Portable Reviewer's guide.

■ The second phase performed a test using EnCase Portable on the Gateway Test PC.

■ The third phase will compare the cloned drive of the test bed vs. the Gateway Test PC drive after EnCase Portable was used to examine this system to determine what, if any, files may have changed as a result of using EnCase Portable.

Phase 1 – Pre-Testing and Familiarization With EnCase Portable

1. The *EnCase Portable Users Guide* and the *EnCase Portable Reviewer's Guide* were reviewed.
2. Following the detailed instructions in the *EnCase Portable Quick Reference Field Guide,* the BIOS (Basic Input Output System) on the Gateway Test PC was set to boot from a USB device. The instructions provided accurate information to access the Gateway computer BIOS by pressing the F1 key as the computer starts. The BIOS was configured to allow USB boot devices and the boot order was set "Removable Device," "CD/DVD ROM," "Hard Drive." The BIOS correctly identified the 3.5-inch floppy drive plugged into the USB ports. The settings were saved and the system was powered off.
3. The EnCase Portable Bootable Security Key was inserted into a USB port on the front of the Gateway Test PC. The powered USB Hub supplied with EnCase Portable v2.1 was plugged into a USB port on the rear of the Gateway Test computer. The 16 GB USB thumb drive supplied with EnCase Portable was plugged into the USB hub for additional data storage capacity as recommended in the EnCase Portable Field Guide.
4. When the computer was powered up, it did not boot from the USB device as expected. The boot sequence defaulted to the hard drive installed in the computer. Research revealed that this particular model Gateway computer and the installed BIOS version will not boot to a USB device, even though the BIOS includes a USB boot option, which was enabled prior to testing.
5. The boot CD supplied with EnCase Portable was inserted into the DVD drive and with the EnCase

Portable Bootable security key inserted in the front USB port. The computer was powered on and a screen displayed "To boot from a CD or DVD press any key." If a key is pressed, the computer boots with CD or DVD in the drive; however, if a key is not pressed in a finite amount of time, the computer will resume its boot order in the BIOS, in this case, the hard drive. A key was pressed and the computer booted to the EnCase Portable CD in the DVD drive. Seven "Out of the Box" tests recommended in the EnCase Portable Reviewer's Guide were performed. Results and observations were:

- The computer boot process and the EnCase Portable application performed slowly when the computer was booted from the EnCase Portable boot CD. It was concluded that EnCase Portable runs from computer memory and the Gateway Test PC was configured with 512mb of RAM, the minimal amount of memory for this computer, resulting in poor performance of EnCase Portable.
- The video display quality was very poor in this operating mode.
- EnCase Portable is configured using the "Source Processor" to create and modify jobs on the Bootable Security Key. Creation and modification of the EnCase Portable jobs requires a computer configured with EnCase Forensic Software and experience using EnCase Forensic software.
- The results for each test are saved in a corresponding folder created on the preconfigured 16 GB memory stick installed in the target computer. Other external USB data storage devices connected to the target computer can also be used to save the test results.
- The "Collect Copy of Drive or Memory" test requires a USB evidence collection drive with sufficient capacity connected to the target computer. A 320GB Toshiba USB external drive was connected to the target computer via the USB hub to collect the results. EnCase Portable created 11 separate files: nine E01 image files (~665Mb), one image file (395MB) and a L01 file (7kb).

Since the Gateway Test PC performed poorly, the same tests were run on an alternate computer, a HP Laptop Computer model G71-347CL, s/n CNF 937BW21, 4gb ram and a 320GB hard drive. An image file of this computer was created to use EnCase Forensics Software to verify any results that EnCase Portable produced. The computer was configured to boot with the Bootable Security Key. This computer performed much faster with increased quality to the display and responsiveness of the user interface. It should be noted that this alternate computer did not contain any contrived data sets specifically designed to test EnCase Portable similar to the Gateway Test PC. Although the performance was noticeably improved, additional digital image files, documents, credit card numbers, date of births and Social Security numbers would provide more realistic scenarios to test the performance increases.

Phase 2 – Triage and Data Collection With EnCase Portable

This phase is actual testing of EnCase Portable Version 2.1 using a known test bed data set:

1. For the initial testing for this section, the "Out of Box" configurations will be used:
   - Collect Document Files: Collects all files designated by EnCase as having the file category of "Document."
   - Collect Mail Files: Collects all files designated by EnCase as having the file category of "Mail."
   - Collect Picture Files: Collects all files designated by EnCase as having the file category of "Picture."
   - Collect Copy of Drive or Memory: Prompts to select physical memory or a storage device and creates an image.
   - Create Internet Artifacts Report: Finds and reports on Internet history, bookmarks, cookies, cached files and downloaded data.

- Create PII Report: Collects information on files found on the system containing personal information. This job searches all document, database and Internet files and identifies Visa, MasterCard, American Express and Discover card numbers, as well as Social Security numbers.
- Triage Pictures: Enables you to preview all picture files and collect selected pictures into a Logical Evidence File (or LEF).[4]

Test 1 – Law Enforcement Use of EnCase Portable Version 2.1

This test was designed to test the scenario of a law enforcement officer serving a search warrant on a suspected gang member to collect all electronic data stored on any computers found on the premises. The out-of-the box tests were performed, the details and time to complete each task are below in Table 1.

TABLE 1. Out of the Box Test Results

Jobs	Start	Stop	Minutes
Collect Documents Files	10:15 a.m.	10:21 a.m.	6
Collect Mail Files	10:26 a.m.	10:28 a.m.	2
Collect Picture Files	10:29 a.m.	10:44 a.m.	15
Create Copy of Drive Memory	10:49 a.m.	12:46 p.m.	117
Collect Internet History	12:51 p.m.	12:53 p.m.	2
Create PII Report	12:55 p.m.	1:13 p.m.	18
Triage Pictures	1:14 p.m.	1:21 p.m.	7

The total time to complete the out of the box test was 2:47. After completion, the reports are displayed and the user can select to save the report as text, rtf, xml or html. The report was saved as html. The drive was hashed using EnCase Portable and the hash matched the hash value from the Tableau TD1 Forensic Duplicator.

[4] EnCase Portable v2.1 Reviewer's Guide 2010

All the reports created were reviewed and verification was made that the tool did collect the evidence requested. The report notes the names and locations of the files on the hard drive. The PII (Personal Identity Information) report did reveal the file containing the generic personal information, where the document was located and in which profile. In this test, EnCase Portable performed as expected.

Test 2 – Configuring a Hash Finder

A known hash value finder can be an efficient way to discover files. Law enforcement can use a hash finder to discover contraband from a suspect's computer. For example, an investigator can use a known hash set of child pornography images and add that set to EnCase Portable's Source manager. EnCase Portable can then identify those files via the hash value.

To configure the job, EnCase v6 is started, a case is opened or new one created, and the source processor is used to configure the new job on the Bootable Security Key. The source processor is located on the lower right side of the EnCase main screen (Figure 1).

After the Source Processor is open, the jobs will be displayed and can be edited. In this case, a new job is to be created using the following steps (Figure 2).

1. Make sure the "Collection Jobs" tab is open.
2. Click on "New."
3. Click on "File Processor."
4. Click on "Hash Finder."
5. Click on "Next."
6. Click on "Create Hash Set."
7. Click on the "Ellipsis Button" to open a box to navigate to the files to be hashed.
8. When finished, click on "OK."

To export the job, the Security Key is plugged into the USB port using the following steps with the Source Processor still open:

1. Click on “Manage EnCase Portable Devices.”
2. Check off the portable device you want to manage (if more than one is plugged in).
3. “Collection Jobs” will appear; check off the job you want to export to the portable device.
4. Click “Export.”

Note – If you only pick one job, that will be the only job on the Bootable Security Key when you finish the export. Export deletes the other “Collection Jobs.” It is a valuable option if the case or search warrant requires that only certain information is to be collected. This will not jeopardize the case by exceeding the scope of the search warrant.

For this test, eight digital images from two users on the computer were placed into the hash value finder. Eight additional images, four from the deleted user Charlie and four that were never placed on the computer, were added to the hash finder to test for false positives. The above procedure was followed in creating the “Hash Finder” collection job.

1. The Bootable Security Key was inserted into one of the front USB ports on the Test Gateway computer.
2. The bootable CD was in the CD/DVD ROM.
3. The computer powered on and booted to the bootable CD.
4. The test was started at 2:18 p.m.
5. The test was completed at 2:37 p.m.

The results of this test were that “Hash Finder” matched eight of the 16 hashes in the data set. The eight that were not found were the four from the deleted user Charlie and the four that never resided on the computer. The “Hash Finder” took a total of 19 minutes. After this test, the Gateway Test PC was powered off.

Test 3 – Triage of Pictures

This test was designed to test the scenario of a parole officer who is visiting one of his parolees. During the visit, the officer inserts EnCase Portable into the parolee’s running computer and initiates a picture triage.

The Bootable Security Key had to be reconfigured to perform this test using the same export procedure in Test 2. This is one of the pre-configured Collection Jobs.

The Gateway Test PC was turned on and booted to one of the cloned hard drives that had been prepared for the testing procedure. The test was performed using the following steps:

FIGURE 1: EnCase Version 6 Source Processor

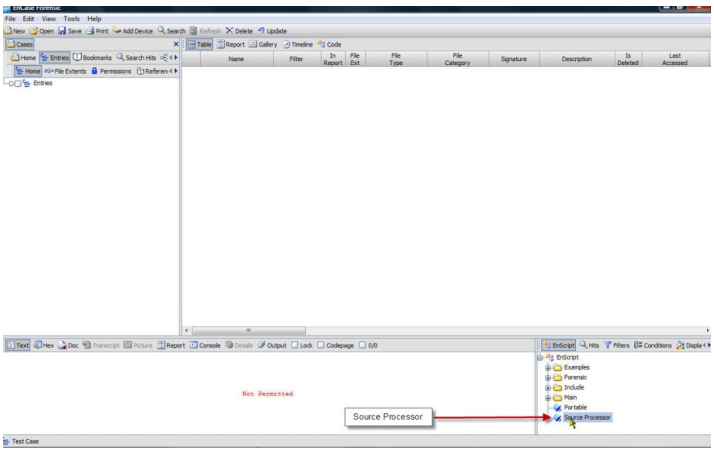
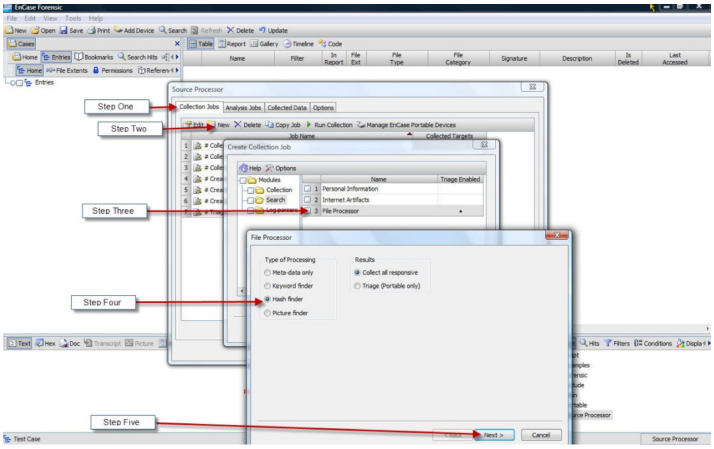


FIGURE 2: Creating a New Job



1. Logged in as Alice.
2. The Bootable Security Key was inserted into the front USB port on the Gateway Test PC at 3:05 p.m.
3. The Bootable Security Key autorun feature initiated and Windows Explorer opened the Bootable Security Key and displays the contents.
4. Clicked on "Run EnCase Portable" to start the EnCase Portable program.
5. A warning appeared indicating that EnCase Portable requires the user to be logged in as an administrator.
6. Logged off the Alice user account.
7. Logged on to the LABGTWY1 administrator account.
8. The Triage test was started at 3:06 p.m.
9. The Triage was finished at 3:33 p.m.
10. Clicking on "Status" and then clicking on "Thumb View" displayed all the digital images on the computer. The images are in thumbnail or gallery view and each has a check box. Eight images were checked and "Collected" to the LEF or Logical Evidence File for later viewing.
11. Total time of test was 27 minutes.
12. Turned off the Gateway Test computer and removed Bootable Security Key.

Test 4 – RAM Collection Test

This test will be conducted on a running computer to simulate an investigator going to a scene and discovering a running computer that may contain evidence.

RAM collection can provide investigators and first responders with the ability to collect vital evidence that resides in the Random Access Memory (RAM), which is lost if a computer loses power (via pulling the plug or proper shutdown). An investigator simply plugs the EnCase Portable Bootable Security Key into a USB port and runs the disk and memory collection process to collect the following:

- Capture opened and minimized screen shots.
- Physical memory.
- Running processes.
- NAS and Steganography files.
- System state.

Lab Computer 2, previously used to create the peer-to-peer file sharing data on the Gateway Test PC, was prepared to perform the EnCase Portable RAM Collection Test using the following steps:

1. LimeWire was launched on Lab Computer 2.
   - Four files, "Ace_Diamond.jpg," "Ace_Heart.jpg," "Ace_Club.jpg" and "Ace_Spade.jpg," were shared on Lab Computer 2.
   - A Gmail e-mail account billygoat49@gmail.com was created.
   - An e-mail was sent to Alice at smitha550@gmail.com from the billygoat49@gmail.com account regarding a conference.
2. On the Gateway Test PC, the Alice user account was accessed and logged on.
   - The LimeWire application on the Gateway test bed computer was accessed and a search was conducted for the four files shared using Lab Computer 2.
   - The four files, "Ace_Heart.jpg," "Ace_Club.jpg," "Ace_Spade.jpg" and "Ace_Diamond.jpg" were identified on LimeWire as being shared by Lab Computer 2.
   - "Ace_Heart.jpg," "Ace_Club.jpg" and "Ace_Spade.jpg" were downloaded using the Alice User Account on the Gateway Test PC.
   - The file "Ace_Diamond.jpg" was downloaded previously by Alice and resides in her My Pictures folder.

3. Logged into Alice Gmail account.
   - ❑ Responded to an e-mail message sent by Billy.
   - ❑ Sent a chat invitation to Billy.
   - ❑ Using Lab Computer 2, Billy replied and a chat session between the Alice and Billy user accounts was conducted between 1:50 and 1:54 p.m. regarding meeting for lunch during the conference.
   - ❑ Logged out of the Alice Gmail account.
4. With the Alice user account still logged onto the Gateway Test PC, Internet Explorer was launched and navigated to the Google search engine main page URL www.google.com.
   - ❑ An Internet search was conducted for "Conference Hotels."
   - ❑ At 2:01 p.m., the search result hyperlink for the Hampton Inn, Manhattan Seaport Financial District was accessed and the process of booking a hotel reservation was simulated.

After Lab Computer 2 was configured, the following steps were performed for the EnCase Portable RAM test:

1. Using a Lab Computer with EnCase v6 and EnCase Portable installed on it, the source processor was accessed to make ensure the jobs were selected and then exported to the EnCase Portable Bootable Security Key.
2. At 9 a.m., the EnCase Portable Bootable Security Key was inserted into the Gateway Test PC.
3. The auto start screen opened a window on the screen enabling the user activate EnCase Portable through a mouse click. The active user account, Alice, was a limited user account and a prompt appeared requesting "Administrator log on Credentials." As confirmed in the earlier 'Triage Test," using EnCase Portable on running computer requires a user account with administrator privileges. Access to an administrator account can be performed when prompted by the EnCase Portable interface or the Windows OS "Switch User" option.
4. On logging into a User Account with Administrator privileges, a window opens identifying the EnCase Portable "Jobs" available. Selection is made by highlighting the job and then clicking "Run Job."
5. In this test, the "Create Copy of Disk or Memory" was highlighted and the "Run Job" was clicked.
6. A window opens and the available disks and memory options are identified as whole drive "0," logical area "C" or the RAM.
7. RAM was selected, "OK" was clicked on and the "Job" started to run.
8. At approximately 9:11 a.m. the collection was completed. Elapsed time for setup and execution of the RAM Collection was approximately 11 minutes.

On completion of the RAM Collection, the results can be examined using EnCase Forensic Software v6.

Updating EnCase Portable

During the course of testing, Guidance Software released an upgrade to EnCase Portable. This upgrade added functionality to process MAC OS computers. The following are the steps taken to upgrade EnCase Portable from v2.1 to v2.2:

1. The new version, v2.2, was downloaded from the Guidance Software website. The download contained the following files:
   - ❑ "EnCase Portable v2.2 field guide."
   - ❑ "EnCase Portable v2.2 release notes."
   - ❑ "EnCase Portable v2.2 user guide."
   - ❑ "Portable v2.2 English Program" ISO file.
   - ❑ "Portable v2.2 Boot CD" ISO file.
   - ❑ "EnCase Portable v2.2 Setup English" .exe file.

- ❑ "EnCase English Restore Portable v2.2 English" .exe file.

2. A new bootable CD and program DVD were created from ISO images.
3. The "EnCase English Restore Portable v2.2" .exe file was used to update the EnCase Portable Bootable Security Key. This process started at 8:30 a.m. and completed at 9:09 a.m. Note: Either the program CD can be used or the .exe file can be used to accomplish this update.

Test 5 – EnCase Portable on a MacBook Pro

A MacBook Pro was used for this test. No extra setup was performed to place known files on the MacBook Pro. This test was used simply to verify EnCase Portable's compatibility with MAC OS. The test was performed with the following steps:

1. The EnCase Portable Bootable Security Key with v2.2 was inserted into the USB port of the MacBook Pro.
2. Powered on MacBook Pro with the EnCase Portable Bootable Security Key v2.2 at 9:19 a.m.
3. Program loaded and the EnCase Portable collection screen appeared at 9:25 a.m.
4. The following jobs were run (Table 2):

TABLE 2. Jobs Run for Test 5

Start Time	Job	End Time
9:34 a.m.	Collect all documents (this process was stopped)	9:45 a.m.
9:55 a.m.	Collect mail	10:06 a.m.
10:08 a.m.	Collect pictures	10:12 a.m.
10:16 a.m.	Collect Internet artifacts	10:20 a.m.

5. Program closed and MacBook powered off.

At the end of each test the results were examined to determine what EnCase Portable found. For this test, the tool did perform as expected in retrieving information from the MacBook Pro.

Test 6 – Triage for Personal Identity Information (PII)

1. The Test Gateway Computer was started. A document file was created using Word Pad, a word processor program included in Windows Operating Systems.
2. The document included several randomly created Social Security numbers using the ###-##-#### format and then copied and pasted several times to make a list. Three phone numbers were randomly created using ###-###-#### format. The document file was saved with the name "Personal" and moved into the "My Documents" folder in the Alice user profile.
3. The test was started at 10:30 a.m. and ended at 10:44 a.m.
4. The results were checked and the document file named "Personal" was found. By highlighting the file in the results and clicking on it, the file opens. The Social Security numbers were highlighted by the EnCase Portable program. The phone numbers were not. Also, in the status section, there was no indication it found phone numbers.
5. In this test, the program did not perform as expected.

Phase 3 – Determining EnCase Portable's Impact on a System

The purpose of this phase is to determine how many and what files are affected when EnCase Portable is plugged into a live system. This will aid an investigation by providing information on what files are changed on a system when the Bootable Security Key is inserted.

Prior to beginning this phase of testing, an exact clone of one of the control "Test Set" hard drives was created using the following steps:

1. A 20 GB test hard drive identical to the control hard drive was wiped and confirmed to be free of data.
2. A clone of the control hard drive was created on the test hard drive using a Tableau TD1 Forensic Duplicator. On completion of this process, the logs were saved and the MD5 Hash values were compared to ensure the two hard drives were identical (see attached logs).
3. Using the Tableau TD1 Forensic Duplicator, image files of the test hard drive were created.
4. The E01 image files were added to EnCase Forensic v6.17.
5. All files are selected in the case by checking off the image.
6. Using the search function with "all files," "create hash" and "verify hash options" checked, the process was started.
7. On completion, the filename, date last accessed, date last modified, date created and hash value fields were selected for export to a comma separated text file for use in the hash result comparison tests.

Three separate tests were performed to determine what files are changed during boot up, an administrator logging in and insertion of the EnCase Portable USB key. After each test, the drive was removed from the Gateway Test PC and imaged using the Tableau TD1 Forensic Duplicator.

To determine what files are changed during a normal boot, the Gateway Test PC was booted to its native operating system. On completion of the boot process, the power was disconnected. Once the computer was off, the hard drive was removed and imaged, and the files were hashed.

To determine what files are changed when a user logs onto the system, the test hard drive was reinstalled into the system and booted up, a user logged into the administrator account, and power was disconnected. The hard drive was removed and imaged, and the files were hashed.

Finally, to determine what files are affected by using the EnCase Portable security key, the hard drive was reinstalled into the system and booted, a user logged into the administrator account, and the EnCase Portable Secure Key was inserted into a USB port. Once the EnCase Portable program completed, loading power to the test bed computer was disconnected. The hard drive was removed and imaged, and the files were hashed.

The Control Hash Set was imported into FTK v1.71. A new case was started with each of the E01 images to index each step in the process. First, the Control Set with just a boot; second, the Control Set with a boot and log on; and third, the Control Set with a boot, logon and starting EnCase Portable USB as a triage tool. The KFF alert was then used to filter out the files that were changed or didn't match the hash set used. Table 3 shows the number of files that matched the KFF Control Hash Set filter and the number of files that were changed.

TABLE 3. Hash Set Files

Files	Total	# Changed
Total Files Hashed and added to the Control Set	44,497	N/A
Control Set with boot	41,439	3,058
Control Set with boot and log on	40,903	3,594
Control Set with boot, log on and EnCase Portable started	40,804	3,693

There were a total of 3,058 files changed during a single boot of the control set: 536 were changed with a single log on and 99 files were changed just inserting the EnCase Bootable Security Key and running the EnCase Portable Program. These files can easily be identified using the data sets.

Conclusion

EnCase Portable can be used in the field to gather information from computers that may contain digital evidence. Since EnCase Portable is configurable by an expert in digital forensics, it can be distributed to non-experts to collect evidence and then returned to the expert for processing. With the exception of EnCase Portable's not correctly identifying phone numbers in the PII test, the tool performed as expected and advertised.

It is important for the user to understand that running computer operating systems are in a constant state of flux. Running processes, even those that are unseen to the user, may change files. For example, inserting a USB drive, such as the one on which EnCase Portable is installed, may cause the operating system to load hardware drivers and save that information for future use. Executing a program such as EnCase Portable will create running processes. These processes will interact with the computer operating system and applications, resulting in files on the computer being changed. Over the course of this test, it was determined that the actions of booting a machine, logging onto the operating system, inserting the EnCase Portable USB stick and executing the program resulted in some changes to files on the computer. After analysis, it was determined that the files that were altered or added as a result of this test were operating system and application files, and not user data.